



**Eur päisches
Patentamt**

**Eur pean
Patent Office**

**Office européen
des brevets**

Bescheinigung

Certificate

Attestation

Die angehefteten Unterla-
gen stimmen mit der
ursprünglich eingereichten
Fassung der auf dem näch-
sten Blatt bezeichneten
europäischen Patentanmel-
dung überein.

The attached documents
are exact copies of the
European patent application
described on the following
page, as originally filed.

Les documents fixés à
cette attestation sont
conformes à la version
initialement déposée de
la demande de brevet
européen spécifiée à la
page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02368110.9

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk



Anmeldung Nr:

Application no.: 02368110.9

Demande no:

Anmeldetag:

Date of filing: 10.10.02

Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

INTERNATIONAL BUSINESS MACHINES CORPORATION

Armonk, NY 10504

ETATS-UNIS D'AMERIQUE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:

(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.

If no title is shown please refer to the description.

Si aucun titre n'est indiqué se référer à la description.)

Method of accessing internet resources through a proxy with an improved security

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s)
revendiquée(s)

Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L29/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of
filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

METHOD OF ACCESSING INTERNET RESOURCES THROUGH A PROXY WITH AN IMPROVED SECURITY

Technical field

5 The present invention relates to the Internet environment wherein a user addresses requests for getting Internet resources to a proxy which transmits these requests to the content server able to provide the Internet resources and relates in particular to a method of accessing Internet resources through a proxy with an improved security.

10

Background

15 The Service Provider market moves up the value chain from pure connectivity services to deliver value-added and revenue generating services. The business model of a Service Provider was initially driven by minutes of use and is being more and more replaced by data traffic generated by users that access to external services, typically not maintained by the Service Provider itself but accessed through the Service Provider platform. The Service Provider plays a key role since it is

the intermediary between the Subscriber and the external services. Its privileged position allows him to not only provide just "simple" access but added value services such as security, single signon, billing, location, etc. at the condition that it cannot be "bypassed" by the user.

In the World Wide Web context where the device being used to access the external Web Services is typically a Web browser, this is usually done through the use of a proxy component, a "Web Proxy", placed in the service provider platform. When the proxy is a forward proxy, the Web browser is enforced to go through the Web proxy by configuration.

When a client program establishes a connection "through" a proxy to a destination content server, it first establishes a connection directly to the proxy server program. The client then negotiates with the proxy server to make the proxy establish a connection on behalf of the client between the proxy and the destination content server. If successful, there are then two connections in place : one between the client and the proxy server and another between the proxy server and the destination content server. Once established, the proxy then receives and forwards traffic bi-directionally between the client and the remote content server. The proxy makes all connection-establishment and packet-forwarding decisions.

A proxy can be configured as "reverse proxy" in order to add more security and to protect in an efficient way the back-end Web services. In such a case, it appears to the client to be the destination content server. To the content server, the reverse proxy server acts as the originator of client requests. If a client wants to access a file, for example main.html, he points its browser to the reverse proxy, www.DomainA.com believing this is the Internet address of the content server. The reverse proxy server will accept the client request for main.html, retrieves the requested page

from the content server residing on w3.DomainB.com, and returns it to the client.

Today, a lot of Web Services use a mechanism called "cookie" to maintain session with the user. Cookies constitute a general mechanism which server side connections can use to both store and retrieve information on the client side of the connection. The addition of a simple, persistent client-side state significantly extends the capabilities of Web based client/server applications. When returning an HTTP object to a client, the server also sends a cookie that the client will store. Included in such a cookie is a domain information indicating in which domain the cookie is valid. Any future HTTP request made by the client which fall in that range will include a transmittal of the current value of the cookie. Although the cookies have become an essential object of every Web connection between a client and a content server, they present an important drawback which is to contain sensitive information that could be potentially used for hacking purpose if they can be received and analyzed by the users themselves.

Summary of the invention

Accordingly, the main object of the invention is to achieve a method of accessing Internet resources through a proxy which keeps the cookies on the service provider platform at the disposal of the proxy thus avoiding these cookies to be downloaded and potentially analyzed by the user or a hacker taking the place of the user.

The invention relates therefore to a method of accessing from an Internet user to Internet resources provided by at least a content server in a data transmission system including a proxy connected to the Internet network, this proxy being provided with authentication means for authenticating the user when receiving a request for Internet resources therefrom, and

wherein the proxy transmits the user request to the content server which sends back a response to the proxy together with at least one cookie containing information about the user's session. This method consists for the proxy receiving the response with the cookie in storing the cookie in a user context database and transmitting this response to the user after the cookie(s) has (have) been removed from the response, so that the user can send all requests for accessing the Internet resources contained in the content server to the proxy

Brief description of the drawings

The above and other objects, features and advantages of the invention will be better understood by reading the following more particular description of the invention in conjunction with the accompanying drawings wherein :

- Fig. 1 is a schematic block-diagram showing a data transmission system implementing the method according to the invention, and
- Fig. 2 is a flow chart of the method of accessing Internet resources through a proxy according to the invention.

Detailed description of the invention

Referring to Fig. 1 representing a data transmission system used in the context of the invention, a service provider provides Web services to a plurality of users such as user 10 through the Internet network 12. Such web services can be any kind of information which can be furnished by a content server 14. When the user wants to access to the content server, he transmits a request to a proxy 16. This proxy has at its disposal a user registry 18 containing the information such as credentials of the users allowed to access the services provided by the service provider (generally the identification

and password of the user). It has also a user context database
20 for each user wherein are stored the session cookies
associated with the user as explained hereunder.

5 As already mentioned, the user's Web browser first establishes
the connection (1) directly to the proxy 16. Then, the proxy
establishes the connection (2) on behalf of user 10 between
proxy 16 and content server 14. Once established, the proxy 16
receives (3) Web response from the content server 14 and
forwards these pages (4) to the user.

10 It must be noted that a session cookie is automatically resent
to the content server when the user requests an URL from this
server. In other words, the cookies are automatically replayed
for the content server whose the Internet Domain matches the
15 full domain name of a server that provided the page which
created the cookie (or cookies) and if they were defined as
valid across this domain. Note that, by default, if the domain
is not specified, a cookie is valid only for the content
server which set it before. It is possible that a small
20 portion of the domain name shares cookies among several
servers sharing a top-level domain. For instance, the cookies
for the "domain A.com" will be resent automatically for the
servers included in the "domainA.com" but will be also resent
for all sub-domain such as "domainAA.domain A.com".

25 The steps of the method according to the invention are now
described in reference to Fig. 2 wherein the proxy device is a
reverse proxy. First of all, it is determined whether the user
context exists when the user gains access to the proxy (step
30). If not, the user logs on to the proxy 16 for accessing an
URL in content server 14, for example the address
30 "w.w.w.domainA.com/serviceB" (step 32). The proxy checks the
credentials sent by the user, either in a form or in the
header of the request such as the HTTP header in the user
registry 18 (step 34). It is then determined whether the

credentials are OK (step 36). If not, the process loops back to the first step. When the credentials are found OK, the proxy creates a user context for this user in the user context database 20 (step 38). Note that, when a user context already exists in the proxy, the request is automatically recognized and mapped by the proxy as a protected URL (it checks if the user has been already authenticated thanks to the presence or not in the user context database of an associated record) that needs to be forwarded to the content server. This implies that all different URLs which access "service B" are defined and mapped in the proxy configuration, such as the address w.w.w.domainA.com/serviceB being mapped with the address w.w.w.domainB.Com. One or several cookies matching the target URL are then added to the request (step 40).

After the user context has been created in the proxy or if it already exists, the request is transmitted by the proxy to the content server with the address w.w.w.domainB.com (step 42). The content server answers back to the proxy with the information requested by the user (step 44). Note that, for various reasons, the content server receiving the request generally needs to track the user session with a unique session ID. But, it can use other mechanisms.

At this stage, the proxy determines whether one or several cookies have been set in the reply sent by the content server (step 46) by checking the statement "set-cookies". When received by the proxy, the cookies are stored in an associated record into the user context (step 48). The cookies are stored with the associated targeted internet domain ("domainB.com") of the content server or with the full content server name ("www.domainB.com") if the domain is not specified, in order to be able to send it again for all HTTP sub-requests. Once the cookies are stored, the statement "set-cookies" is removed from the HTTP response (step 50). So, it hides to the user the

value of the cookie thereby adding more security to the system.

Then, the HTTP reply is sent back to the user browser without any cookies referencing the content server (step 52). It is
5 then checked whether there are other user requests to same content server (step 54). If not, the session is ended (step 56). When there are other subsequent requests to the same URL, the process loops backs to the beginning (step 30).

Although the method according to the invention can be applied
10 with a forward proxy, it is preferable to use a proxy configured as a reverse proxy. But, without the invention, there is problem if the content server is not in the same Internet domain as the proxy. In such a case, the user should receive an answer from the server with a cookie valid for the
15 domain to which belongs the server (e.g. domainB.com) but invalid for his own domain (e.g. domainA.com). Since the name of the server is for the user's browser a name of its domain (domainA.com) the cookie will not be sent to the proxy for subsequent sub-requests to the same URL. Therefore, the
20 session will not be maintained.

Conversely, if the method according to the invention is used with a reverse proxy, this one receives the cookie in the domain of the content server (e.g. domainB.com) and stores it into the user context database. When subsequent sub-requests
25 to the same URL are sent to the reverse proxy, the latter retrieves the cookie to be sent to the content server in as much as it establishes a correspondence between the URL seen by the user's browser in a first domain (e.g. domainA.com) and the true name of the server in a second domain (e.g.
30 domainB.com). In such a case, the session will be maintained.

CLAIMS

1. Method of accessing from an Internet user (10) to Internet resources provided by at least a content server (14) in a data transmission system including a proxy (16) connected to the Internet network (12), said proxy being provided with authentication means (18) for authenticating said user when receiving a request for Internet resources therefrom, and wherein said proxy transmits the user request to said content server which sends back a response to the proxy together with at least one cookie containing information about said user ;
- Said method being characterized in that it consists for the proxy receiving said response with said cookie in storing said cookie in a user context database (20) and transmitting said response to said user after said cookie has been removed from said response, so that said user can send all subsequent requests for accessing said Internet resources contained in said content server to said proxy.
2. Method according to claim 1, wherein said proxy (16) is configured as a reverse proxy establishing the connexion to said content server (14) on behalf of said user (10) when receiving said request from said user, whereby said cookie is transmitted by said reverse proxy to said content server when said user sends other requests for the same URL even if said content server does not belong to the same domain as said reverse proxy.
3. Method according to claim 1 or 2, wherein said cookie which has been stored in said user context is added to all subsequent requests from said user (10) for accessing Intranet resources in said content server (14).

4. Method according to claim 3, wherein the response from said content server (14) to said proxy (16) includes a statement "set-cookies", said statement being removed from said response before transmitting it to said user (10).
5. System comprising means adapted for implementing the method according to any one of claims 1 to 4.

METHOD OF ACCESSING INTERNET RESOURCES THROUGH A PROXY WITH AN IMPROVED SECURITY

Abstract

5 method of accessing from an Internet user (10) to Internet
resources provided by at least a content server (14) in a data
transmission system including a proxy (16) connected to the
Internet network, this proxy being provided with authentication
means (18) for authenticating the user when receiving a request
for Internet resources therefrom, and wherein the proxy
10 transmits the user request to the content server which sends
back a response to the proxy together with at least one cookie
containing information about the user. This method consists
for the proxy receiving the response with the cookie in storing
the cookie in a user context database (20) and transmitting
15 this response to the user after the cookie has been removed
from the response, so that the user can send all requests for
accessing the Internet resources contained in the content
server to the proxy

FIG. 1

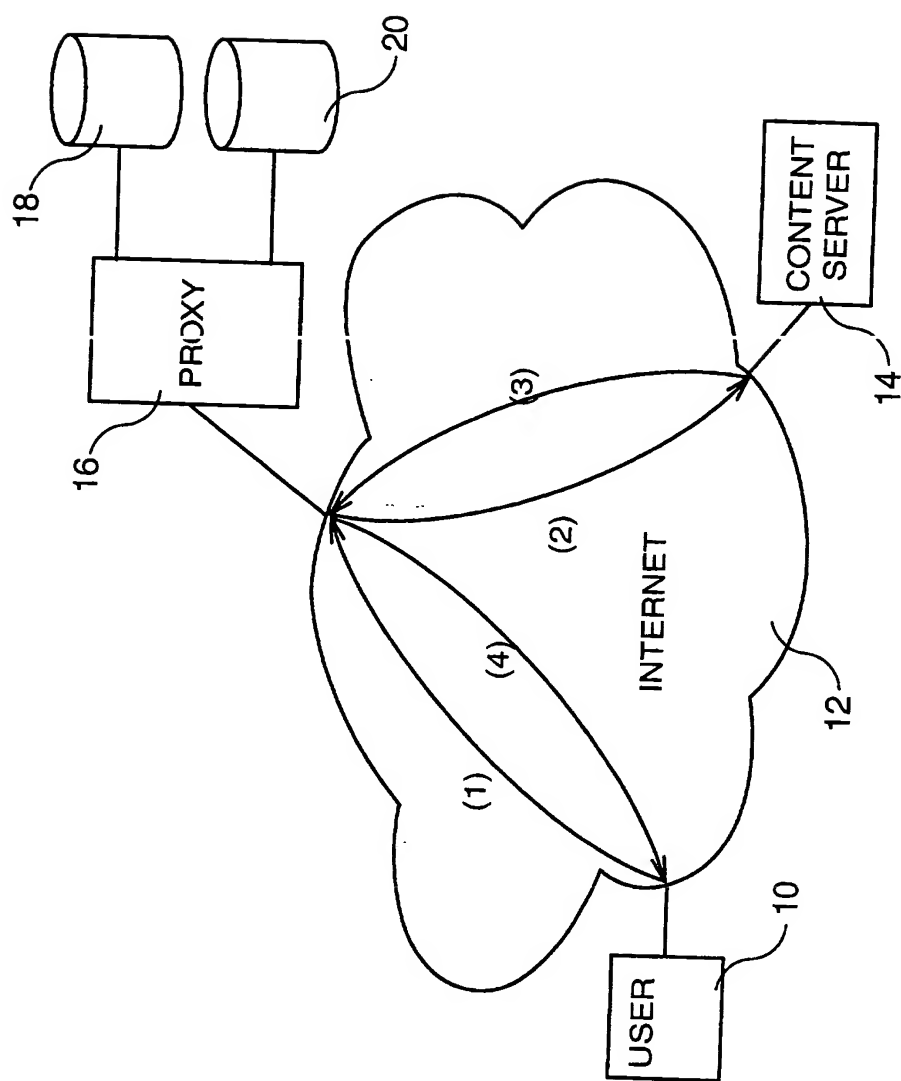


FIG. 1

